EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	113	(380/263).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/20 16:08
S3	13	quantum adj encryption and optical adj pulses	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 17:03
S4	13	quantum adj encryption and optical adj pulse	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 15:02
S5	117465	"1" and (authenticat$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 16:08
S6	113	(380/263).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/20 16:08
S7	34	S6 and (authenticat$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 16:12
S8	9	S6 and (authenticat$3) and quantum	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 16:12
S9	11	quantum adj encryption and phase adj modulation	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 21:06
S10	1	("6778669").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/20 17:10
S11	5503	polarization and phase adj modulation	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 17:21

EAST Search History

S12	372	(polarization same phase adj modulation) and quantum	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 17:26
S13	2	(polarization same phase adj modulation) and quantum adj encryption	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 18:59
S14	11	(phase adj modulation) and quantum adj encryption	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 17:29
S15	11	quantum adj encrypt$3 and (horizontal with vertical)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 17:34
S16	329	polarization adj rotator and quantum	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 17:34
S17	2	polarization adj rotator and quantum adj encrypt$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 17:37
S18	6	rotator and quantum adj encrypt$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 17:38
S19	7	rotat$3 with angle and quantum adj encrypt$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 21:03

EAST Search History

S20	0	mach adj zehnder adj interferomeeter	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 21:03
S21	398	lithium adj niobate adj modulator	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 21:04
S23	1	lithium adj niobate adj modulator and quantum adj encrypt$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 21:04
S24	23	quantum adj encryption and phase adj modulat$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 21:06
S25	0	quantum adj encrypt$3 and message adj authentication adj code	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 15:20
S26	99	message adj authentication adj code near4 (generate derive) near4 key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/20 22:55
S27	25	(optic$3) near4 encrypt$3 and message adj authentication adj code	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 16:47
S28	14	(optic$ qubit) same message adj authentication adj code	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 16:52

S29	0	(message adj authentication adj code mac) with authenticate near4 channel	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 16:52
S30	0	(message adj authentication adj code mac) with authenticating near4 channel	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 16:52
S31	924	(message adj authentication adj code mac) with signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 16:56
S32	667	(message adj authentication adj code mac) with signature same authenticat$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 16:56
S33	649	(message adj authentication adj code mac) with signature same authenticat$3	US-PGPUB; USPAT	OR	ON	2007/07/21 16:57
S34	197	(message adj authentication adj code mac) with signature same authenticat$3	USPAT	OR	ON	2007/07/21 16:58
S35	47	(message adj authentication adj code mac) with password same authenticat$3	USPAT	OR	ON	2007/07/21 16:58
S36	37	bb84 same phase	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 19:00
S37	16	bb84 same phase same polarization	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 19:00

EAST Search History

S38	16	bb84 same phase same (polariz$2 polarization)	US-PGPUB;
			USPAT;
			USOCR;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/07/21 19:00

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

+quantum +encryption +authentication SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used: **quantum encryption authentication**

Found **58** of **207,474**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 58

Result page: **1** 2 3 next

Relevance scale

1 Special section on impact of quantum technologies on networks and networking research: Quantum-noise: protected data encryption for WDM fiber-optic networks

Eric Corndorf, Chuang Liang, Gregory S. Kanter, Prem Kumar, Horace P. Yuen

October 2004 **ACM SIGCOMM Computer Communication Review**, Volume 34 Issue 5

Publisher: ACM Press

Full text available: pdf(696.74 KB) Additional Information: full citation, abstract, references, index terms

We demonstrate high data-rate quantum-noise{protected data encryption through optical fibers using coherent states of light. Specifically, we demonstrate 650Mbps data encryption through a 10Gbps data-bearing, in-line amplified 200km-long line. In our protocol, legitimate users (who share a short secret-key) communicate using an M-ry signal set while an attacker (who does not share the secret-key) is forced to contend with the fundamental and irreducible quantum-measurement noise of coherent stat ...

Keywords: data encryption, quantum cryptography

2 Miscellany: Quantum cryptography in practice

Chip Elliott, David Pearson, Gregory Troxel

August 2003 **Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '03**

Publisher: ACM Press

Full text available: pdf(809.93 KB) Additional Information: full citation, abstract, references, citings, index terms

BBN, Harvard, and Boston University are building the DARPA Quantum Network, the world's first network that delivers end-to-end network security via high-speed Quantum Key Distribution, and testing that Network against sophisticated eavesdropping attacks. The first network link has been up and steadily operational in our laboratory since December 2002. It provides a Virtual Private Network between private enclaves, with user traffic protected by a weak-coherent implementation of quantum cryptogra ...

Keywords: IPsec, cryptographic protocols, error correction, key agreement protocols, privacy amplification, quantum cryptography, quantum key distribution, secure networks

3 Wireless network security I: Application of synchronous dynamic encryption system in mobile wireless domains

Hamdy S. Soliman, Mohammed Omari
October 2005 **Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks Q2SWinet '05**
Publisher: ACM Press
Full text available: pdf(159.81 KB) Additional Information: full citation, abstract, references, index terms

Motivated by the tradeoff between security and efficiency performance parameters that has been imposed on all modern wireless security protocols, we designed a novel security system that gained in both parameters. Our system is based on stream ciphers for their speed, but maintaining a much more solid and proven security. Such security strength stems from the novel deployment of permutation vectors and the data records in the regeneration of the secret key. Moreover, the involvement of the forme ...

Keywords: dynamic encryption, flexible integrity, integrity violations, mobile network security, permutation vectors, seamless handover

4 Session 3: Detectable byzantine agreement secure against faulty majorities
Matthias Fitzi, Daniel Gottesman, Martin Hirt, Thomas Holenstein, Adam Smith
July 2002 **Proceedings of the twenty-first annual symposium on Principles of distributed computing PODC '02**
Publisher: ACM Press
Full text available: pdf(1.06 MB) Additional Information: full citation, abstract, references, citings

It is well-known that *n* players, connected only by pairwise secure channels, can achieve Byzantine agreement only if the number *t* of cheaters satisfies *t* < *n*/3, even with respect to computational security. However, for many applications it is sufficient to achieve *detectable broadcast.* With this primitive, broadcast is only guaranteed when all players are non-faulty ("honest"), but all non-faulty players always reach agreement on whether broadcast was achiev ...

Keywords: broadcast, byzantine agreement, multi-party computation, public-key infrastructure, quantum signatures

5 Authentication & trust management: Unconditionally secure ring authentication
Reihaneh Safavi-Naini, Shuhong Wang, Yvo Desmedt
March 2007 **Proceedings of the 2nd ACM symposium on Information, computer and communications security ASIACCS '07**
Publisher: ACM Press
Full text available: pdf(322.39 KB) Additional Information: full citation, abstract, references, index terms

We propose ring authentication in unconditionally secure setting. In a ring authentication system a sender can choose a set of users and construct an authenticated message for a receiver such that the receiver can verify authenticity of the message with respect to the user group chosen by the real sender. The sender will be unconditionally secure even if the receiver has corrupted up to *c* users and has access to up to &ell; past messages in the system. This functionality is similar to ...

Keywords: authentication codes, ring signature, unconditional security

6 Quantum cryptography: A survey
Dagmar Bruss, Gábor Erdélyi, Tim Meyer, Tobias Riege, Jörg Rothe
July 2007 **ACM Computing Surveys (CSUR)**, Volume 39 Issue 2
Publisher: ACM Press
Full text available: pdf(335.26 KB) Additional Information: full citation, abstract, references, index terms

We survey some results in quantum cryptography. After a brief introduction to classical cryptography, we provide the quantum-mechanical background needed to present some fundamental protocols from quantum cryptography. In particular, we review quantum key distribution via the BB84 protocol and its security proof, as well as the related quantum bit commitment protocol and its proof of insecurity.

Keywords: Quantum bit commitment, quantum cryptography, quantum key distribution

7 Privacy and security in highly dynamic systems: Perspectives for cryptographic long-term security
Johannes Buchmann, Alexander May, Ulrich Vollmer
September 2006 **Communications of the ACM**, Volume 49 Issue 9
Publisher: ACM Press
Full text available: pdf(94.37 KB) html(24.85 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic long-term security is needed, but difficult to achieve. Use flexible cryptographic tools, and have replacements ready.

8 Quantum "encryption" (student paper panel)
Mark V. Hurwitz
April 2000 **Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions CFP '00**
Publisher: ACM Press
Full text available: pdf(107.79 KB) Additional Information: full citation, references, index terms

9 Practical byzantine fault tolerance and proactive recovery
Miguel Castro, Barbara Liskov
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press
Full text available: pdf(1.63 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement re ...

Keywords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine replication, state transfer

10 Multicast security and its extension to a mobile environment
Li Gong, Nachum Shacham
August 1995 **Wireless Networks**, Volume 1 Issue 3
Publisher: Kluwer Academic Publishers
Full text available: pdf(1.22 MB) Additional Information: full citation, abstract, references, citings

Multicast is rapidly becoming an important mode of communication and a good platform for building group-oriented services. To be used for trusted communication, however, current multicast schemes must be supplemented by mechanisms for protecting traffic, controlling participation, and restricting access of unauthorized users to data exchanged by the participants. In this paper, we consider fundamental security issues in building a trusted multicast facility. We discuss techniques for group- ...

11 CryptoManiac: a fast flexible architecture for secure communication
Lisa Wu, Chris Weaver, Todd Austin
May 2001 **ACM SIGARCH Computer Architecture News , Proceedings of the 28th annual international symposium on Computer architecture ISCA '01**, Volume 29 Issue 2
Publisher: ACM Press
Full text available: pdf(836.04 KB) Additional Information: full citation, abstract, references, citings, index terms

The growth of the Internet as a vehicle for secure communication and electronic commerce has brought cryptographic processing performance to the forefront of high throughput system design. This trend will be further underscored with the widespread adoption of secure protocols such as secure IP (IPSEC) and virtual private networks (VPNs).

In this paper, we introduce the CryptoManiac processor, a fast and flexible co-processor for cryptographic workloads. Our design is extreme ...

12 Book reviews: Review of "Data Privacy and Security by David Salomon"; Spring-Verlag, 2003, $51.48, Hardcover.
Nick Papanikolaou
June 2005 **ACM SIGACT News**, Volume 36 Issue 2
Publisher: ACM Press
Full text available: pdf(2.56 MB) Additional Information: full citation, abstract, references, index terms

The field of cryptology and data security hardly needs any introduction; numerous popular accounts of the subject have appeared over the years, and it is already a core topic in undergraduate computer science. The very term "cryptology" is testimony to the long history of the field; the term is derived from the words κσνπτós (meaning hidden), and λóγos (meaning speech), which have retained their meaning in the Greek language for many centuries.

13 Security Mechanisms in High-Level Network Protocols
Victor L. Voydock, Stephen T. Kent
June 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 2
Publisher: ACM Press
Full text available: pdf(3.23 MB) Additional Information: full citation, references, citings

14 Intercepting mobile communications: the insecurity of 802.11
Nikita Borisov, Ian Goldberg, David Wagner
July 2001 **Proceedings of the 7th annual international conference on Mobile computing and networking MobiCom '01**
Publisher: ACM Press
Full text available: pdf(181.52 KB) Additional Information: full citation, abstract, references, citings, index terms

The 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol, used to protect link-layer communications from eavesdropping and other attacks. We have discovered several serious security flaws in the protocol, stemming from mis-application of cryptographic primitives. The flaws lead to a number of practical attacks that demonstrate that WEP fails to achieve its security goals. In this paper, we discuss in detail each of the flaws, the underlying security princip ...

15 An introduction to quantum cryptography
Nick Papanikolaou
May 2005 **Crossroads**, Volume 11 Issue 3
Publisher: ACM Press
Full text available: html(40.57 KB) Additional Information: full citation, references, index terms

16 A new family of authentication protocols
Ross Anderson, Francesco Bergadano, Bruno Crispo, Jong-Hyeon Lee, Charalampos Manifavas, Roger Needham
October 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 4
Publisher: ACM Press
Full text available: pdf(821.42 KB) Additional Information: full citation, abstract, citings, index terms

We present a related family of authentication and digital signature protocols based on symmetric cryptographic primitives which perform substantially better than previous constructions. Previously, one-time digital signatures based on hash functions involved hundreds of hash function computations for each signature; we show that given online access to a timestamping service, we can sign messages using only two computations of a hash function. Previously, techniques to sign infinite streams invol ...

Keywords: authentication, hashing, non-repudiation, timestamping

17 A fuzzy commitment scheme
Ari Juels, Martin Wattenberg
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press
Full text available: pdf(966.08 KB) Additional Information: full citation, abstract, references, citings, index terms

We combine well-known techniques from the areas of error-correcting codes and cryptography to achieve a new type of cryptographic primitive that we refer to as a fuzzy commitment scheme. Like a conventional cryptographic commitment scheme, our fuzzy commitment scheme is both concealing and binding: it is infeasible for an attacker to learn the committed value, and also for the committer to decommit a value in more than one way. In a convent ...

18 Radio-layer security: Securing wireless systems via lower layer enforcements
Zang Li, Wenyuan Xu, Rob Miller, Wade Trappe
September 2006 **Proceedings of the 5th ACM workshop on Wireless security WiSe '06**
Publisher: ACM Press
Full text available: pdf(348.47 KB) Additional Information: full citation, abstract, references, index terms

Although conventional cryptographic security mechanisms are essential to the overall problem of securing wireless networks, these techniques do not directly leverage the unique properties of the wireless domain to address security threats. The properties of the wireless medium are a powerful source of domain-specific information that can complement and enhance traditional security mechanisms. In this paper, we propose to utilize the fact that the radio channel decorre-lates rapidly in space, tim ...

Keywords: authentication, confidentiality, fading, key establishment, propagation, wireless channel estimation

19 Some facets of complexity theory and cryptography: A five-lecture tutorial

Jörg Rothe

December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4

Publisher: ACM Press

Full text available: pdf(2.78 MB) Additional Information: full citation, abstract, references, citings, index terms, review

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

20 Academic papers: A cryptography course for non-mathematicians

Rich Schlesinger

October 2004 **Proceedings of the 1st annual conference on Information security curriculum development InfoSecCD '04**

Publisher: ACM Press

Full text available: pdf(104.04 KB) Additional Information: full citation, abstract, references, index terms

Traditionally, courses in cryptography have been heavily mathematical in nature. Yet, there is a large population of Information Systems practitioners who are not mathematicians, but who need to implement cryptography as a part of an overall system that they are developing. These people need a thorough understanding of the characteristics of good cryptographic communication protocols. Without this level of understanding, numerous cryptosystems have been deployed that use proper encryption algori ...

Keywords: cryptography

Results 1 - 20 of 58 Result page: **1** 2 3 next